REMARKS

Claims 1-28 are pending in this application. Claims 1 and 5 have been amended for minor corrections. No new matter has been added.

Claims 1-8, 10-15, 17-19, 21-25, 27-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,818,936 to Mashayekhi in view of U.S. Patent No. 5,761,309 to Ohashi et al. Applicants respectfully traverse the rejection.

The Examiner relied upon Figs. 2, 4A, 4B and their corresponding description in Mashayekhi, and the background and Fig. 11 of Ohashi et al. in rejecting independent claim 1. Applicants respectfully disagree with the Examiner's application of the cited references.

The Examiner stated in item (1) on page 2 of the Office Action that the "group certificate issuing apparatus" recited in claim 1 is substantially disclosed as a "certificate authority (CA)" 220 in Fig. 2 of Mashayekhi. But concurrently, in item (2) on page 2 of the Office Action, the Examiner relied upon the operation of the "database API" 206 as disclosure of the operation of "group certificate issuing apparatus" recited in claim 1.

Thus, the Examiner cited two separate and distinct components shown in Fig. 2 of Mashayekhi, neither of which resides on the client side ("certificate authority" 220 being its own node and "database API" 206 residing in server node 202a), as disclosure of:

> "a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs when there is said remote processing request and a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server,"

as recited in claim 1. (Emphasis added)

Furthermore, the Examiner in item (2) on pages 2-3 of the Office Action stated that "the database API 206 accesses the authentication database 204 and provides an encrypted application

secret along with the private key for decrypting the secret." Applicants respectfully submit that

the group certificate, as recited in claim 1, is not analogous to the "encrypted application secret

along with the private key for decrypting the secret." Applicants refer to step s1 of Fig. 2, Fig.

12, and their corresponding description in the specification for an illustrative embodiment of

group certificate as claimed. For example, group certificate may include "original group

information added with issue side processed value obtained by an encryption of the original

group information using cryptographic function. The "encrypted application secret" described in

Mashayekhi, on the other hand, is not obtained by encrypting the private key. As such, the cited

portions of Mashayekhi, as relied upon by the Examiner, further fails to disclose or suggest,

> "said group certificate issuing apparatus adds an issuance side processed value
> obtained by encrypting the information of the original group information by a
> cryptographic function to the original group information and defines this as the
> group certificate...,"

as recited in claim 1. (Emphasis added)

With respect to the user login step 404 of Mashayekhi, discussed by the Examiner in item

(3) on page 3 of the Office Action, it appears to merely relate to a network client login

authentication step. (please see col. 7, lines 1 and 20-22 of Mashayekhi) As such, this user login

authentication does not appear to teach or suggest any authentication using a group certificate.

Applicants, therefore, respectfully submit that Mashayekhi, as relied upon by the

Examiner, fails to disclose or suggest the above-cited features of claim 1.

The Examiner acknowledged that Mashayekhi further fails to disclose "performs said

authentication by confirming that said issuance side processed value and said verification side

processed value coincide," and relied upon Ohashi et al. as a combining reference to address

only this feature. As such, applicants respectfully submit that even assuming, arguendo, that it

would be obvious to the skilled artisan to combine the references as proposed by the Examiner, the combination would fail to teach or suggest the above-discussed features of claim 1.

And regarding the Examiner's application of Ohashi et al., the cited portions thereof (col. 1, lines 4-6 and 10-13, and col. 13, lines 6-10) appear to describe a server side authentication technique where a response Res, which is generated using a user secret key Ku stored in a smart card and a random number retrieved from the server side, is compared to a Res', which is generated using the same secret key Ku retrieved from a database using the card number of the smart card provided at the beginning of the process. (See, e.g., Fig. 7 and col. 12, lines 55-67 of Ohashi et al.) As such, the technique in Ohashi et al. does not appear to teach or suggest generating a "verification side processed value," on the server side, by processing any part of the group certificate received from the client side (or smart card) "by [a] cryptographic function to obtain a verification side processed value." Applicants, therefore, respectfully submit that even assuming, arguendo, that it would be obvious to the skilled artisan to combine Mashayekhi and Ohashi et al. in the manner proposed by the Examiner, the combination would fail to teach or suggest,

> "said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide,"

as recited in claim 1. (Emphasis added)

Accordingly, applicants respectfully submit that independent claim 1, together with claims 2-3 dependent therefrom, are patentable over Mashayekhi and Ohashi et al. individually and in combination. Independent claims 4-6 include limitations similar to those discussed above

of claim 1, and are, therefore, together with claims 7-8, 10-15, 17-19, 21-25, and 27-28 dependent therefrom, patentable for at least the same reasons.

Claims 9, 16, 20, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,818,936 to Mashayekhi in view of U.S. Patent No. 5,761,309 to Ohashi et al., further in view of U.S. Patent No. 5,892,828 to Perlman. Applicants respectfully traverse the rejection.

The Examiner appears to have relied upon Perlman to disclose "the detail of the hash algorithm" that "has not been shown precisely" in Mashayekhi. (Page 9 of the Office Action) Therefore, the further combination of Perlman, as applied by the Examiner, would not teach or suggest the features of claim 1 discussed above even if such combination were obvious to the skilled artisan. Claims 9 and 16 depend from claim 5, and claims 20 and 26 depend from claim 6. As such, they are patentable over the cited references for at least the same reasons.
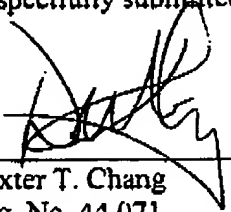
Statements appearing above in respect to the disclosures in the cited references represent the present opinions of the undersigned attorney and, in the event that the Examiner disagrees with any of such opinions, it is respectfully requested that the Examiner specifically indicate those portions of the respective reference providing the basis for a contrary view.

The Examiner has made of record, but not applied, several U.S. patents. Applicants appreciate the Examiner's implicit finding that these references, whether considered alone or in combination with others, do not render the claims of the present application unpatentable.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

84050361_1   13

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,

Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.:   100794-11702 (FUJA 18.671)
DTC:fd

84050301_1   14